FortiAuthenticator™ Token Based SSL VPN

Solution Guide

FortiAuthenticator™ Token Based SSL VPN Solution Guide

October 23, 2013

Revision 1

Technical Documentation	http://help.fortinet.com
Knowledge Base	http://kb.fortinet.com
Forums	https://support.fortinet.com/forums
Customer Service & Support	https://support.fortinet.com
Training	http://training.fortinet.com
FortiGuard Threat Research & Response	http://www.fortiguard.com
License Agreement	http://www.fortinet.com/doc/legal/EULA.pdf
Document Feedback	Email: techdocs@fortinet.com

Table of contents

Change Log

Revision	Date	Change Description
1	2013-10-23	Initial revision

Introduction

This document provides a configuration guide for setting up token based SSL VPNs using the FortiGate and the FortiAuthenticator. The guide provides a step by step walkthrough on both the FortiAuthenticator and the FortiGate, however, for a detailed understanding on the token algorithms and seed handling further reading is required, as the objective of this guide is to provide a configuration walkthrough.

Software Versions

The configuration discussed in this document was tested on the following firmware versions:

- FortiAuthenticator 3.0
- FortiOS 5.0 GA Patch Release 4

FortiAuthenticator Token Based SSL VPN Guide

Introduction

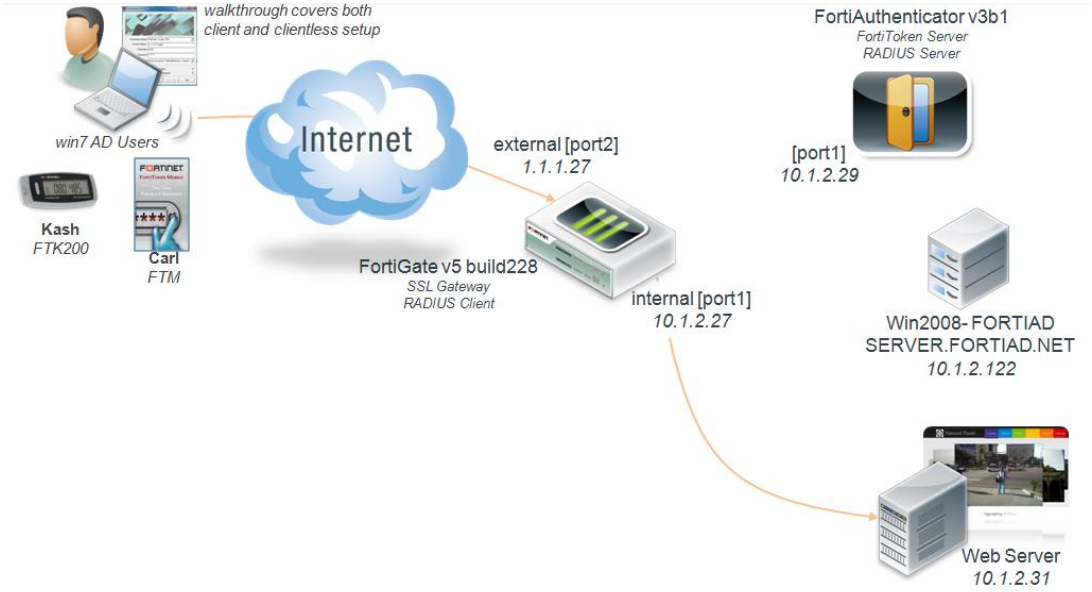
The purpose of this document is to provide a step by step configuration guide on how to setup token based SSL VPNs, using the FortiGate and the FortiAuthenticator. The intention is to provide a concise configuration walkthrough which will allow for the successful deployment of token based VPNs.

The guide will step through the FortiAuthenticator configuration before moving on the FortiGate, before finally testing the setup. All the topology components are using factory default settings, except for the IP configuration, which is already in place.

Note: Before commencing the configuration, please ensure that the date and time are correctly configured and synchronised across all of the topology elements.

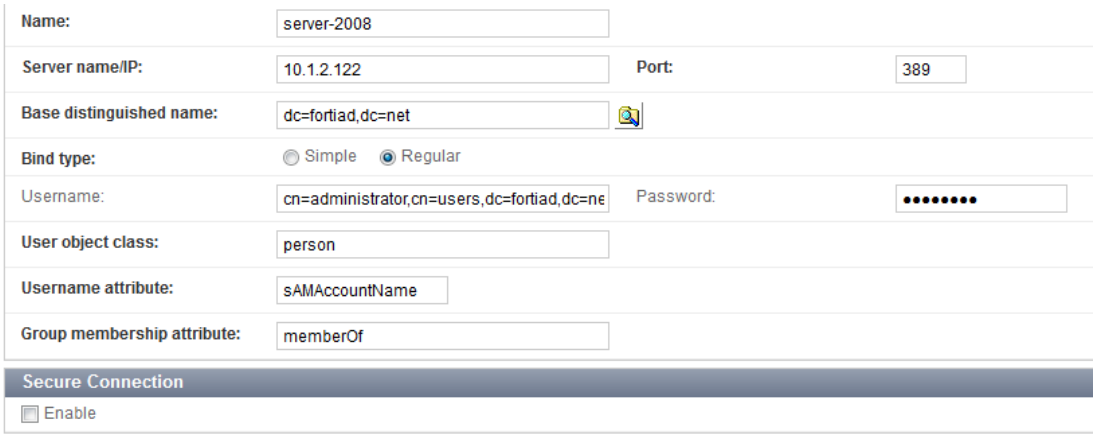
If the intention is to use the FortiToken Mobile, please ensure that this is downloaded and installed on the relevant mobile device.

Topology



FortiAuthenticator Directory Services Configuration

To commence the configuration on the FortiAuthenticator, the remote user directory services and tokens must be added. Firstly the remote AD/LDAP server must be configured. Within the user interface, under *Authentication>Remote Auth. Servers>LDAP*, click on ***Create New***, then complete the AD server settings in a format similar the output below.



The username and password required does not necessarily have to be an administrator; the user only requires enough rights to browse the directory for the purposes of pulling users and groups from the directory, into the FortiAuthenticator.

The 'Windows Active Directory Domain Authentication' section does not have to be completed as a requirement for this configuration.

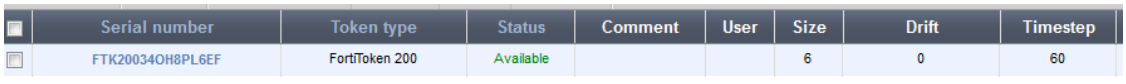
Once the details have been entered, ***Click*** on the folder icon (next to the base distinguished name field) to ensure that you can browse the directory. If the directory is accessible, then close the browsing window and click on ***OK***.

The next step is to import the user (the one intended for SSL remote access) from the directory to the FortiAuthenticator. The user must be in place on the FortiAuthenticator as in the current version (v3.0), unknown user authentication is not supported.

In the user interface go to *User Management>Remote Users* and click on ***Import***, then select the relevant pre-defined remote LDAP server and click on import users. From the pop-up window select the relevant user(s) and click on ***OK***. The remote user(s), should appear as follows.

FortiAuthenticator Adding Tokens

The next step is to import the tokens into the FortiAuthenticator. Under *User Authentication>User Management>FortiTokens* click on ***Create New***. If importing FortiToken200's, then enter the serial number and click on ***OK***. At this point the FortiAuthenticator will attempt to access the FortiGuard cloud services and download and install the unique seed associated with the token serial number (the seed is also removed from FortiGuard with this process). The seed download from the FortiGuard cloud is the default import method, it is also possible to order a secure CD with the seed. A successfully imported FortiToken200 should be viewable as follows.

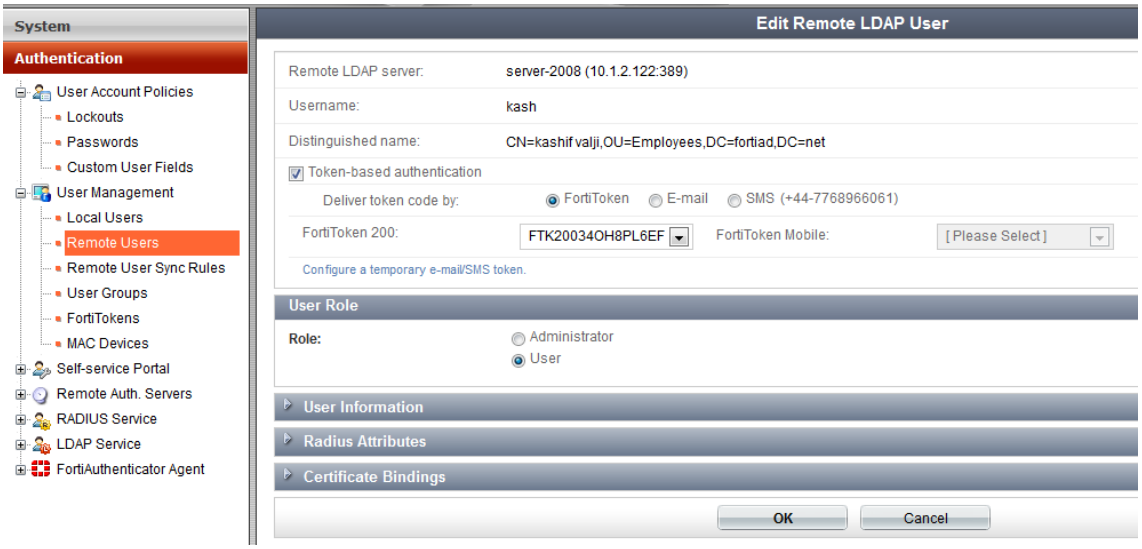


Click on the ***Token Serial Number*** to edit the Token and from the edit settings click on '***Synchronize***' to synchronise the token. This step is essential to ensure that the token and the FortiAuthenticator are in sync.

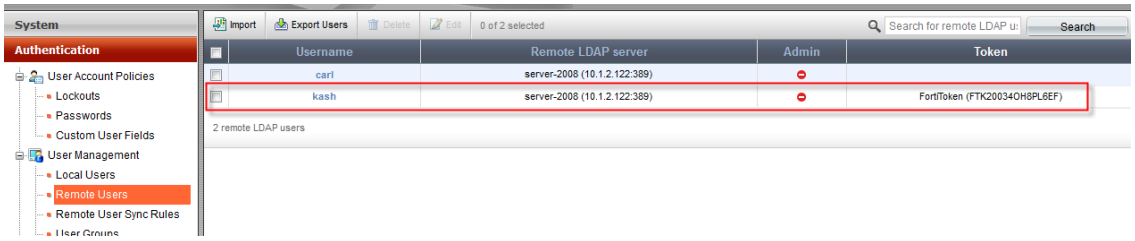
If using the FortiToken Mobile (FTM), then the available licenses should be viewable under *Authentication* > *User Management* > *FortiTokens*, the FTM tokens are added based on a license file, which is uploaded via *System* > *Administration* > *Licensing*. No steps are required with the FortiToken Mobile just yet, other than ensuring that the licenses are visible.

FortiAuthenticator Assigning Tokens

Once the relevant users and tokens have been imported into the FortiAuthenticator the two elements must linked together. The process for assigning a FortiToken200 is as follows; within the FortiAuthenticator interface go to *User Management* > *Remote Users* and click on the ***username*** the token will be assigned to. From the user edit view check the Token-Based authentication tick box, select FortiToken and apply the relevant token from the FortiToken 200 drop down list (as shown below). If the user settings are correct then click on ***OK***.

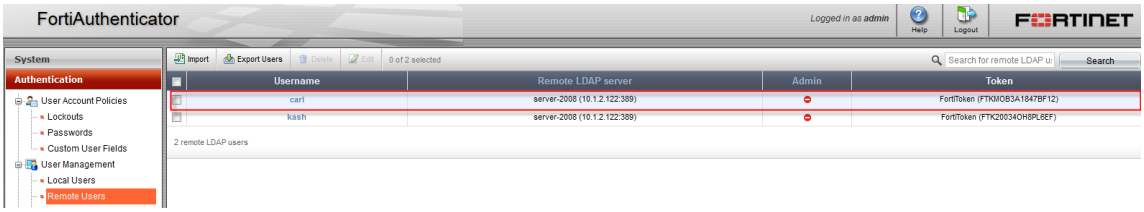


A successfully assigned FortiToken200 user should be viewable as below.

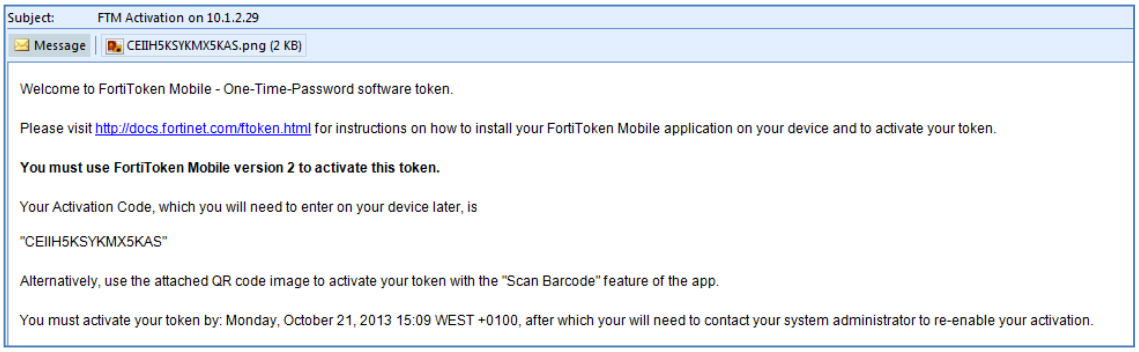


To assign FortiToken Mobile; within the FortiAuthenticator interface go to *User Management* > *Remote Users* and click on the username the token will be assigned to. From the user edit view check the Token-Based authentication tick box, select FortiToken and apply the relevant token from the FortiToken Mobile drop down list. Ensure that the user has a valid email address configured under the *'User Information'* section and that the FortiAuthenticator has the appropriate mail server configuration to email the activation code to the user. It is also possible to send the activation code through SMS, however this requires a valid SMS server such as FortiGuard SMS which requires a valid license. If the user settings are correct then click on ***OK***. At this point, the FTM activation code will be sent to the user via e-mail or SMS.

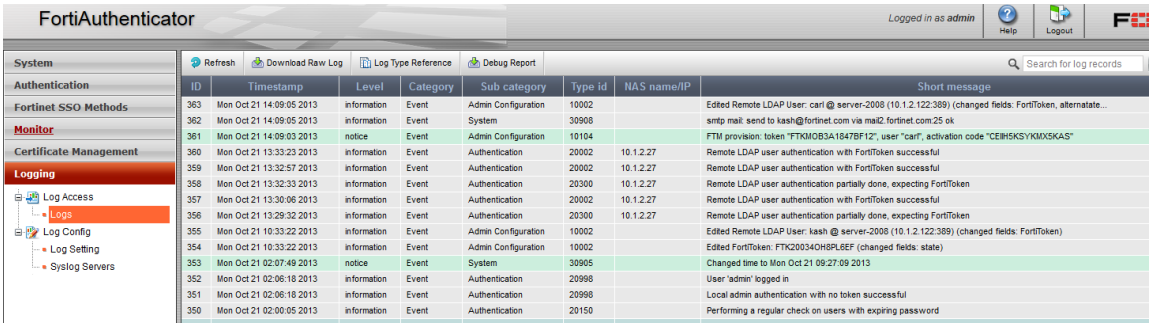
An Active Directory imported user with a FTM assigned should be viewable as follows under *Authentication>User Management>Remote Users.*



The FTM user should receive an email with the FTM activation code, this should be as follows.



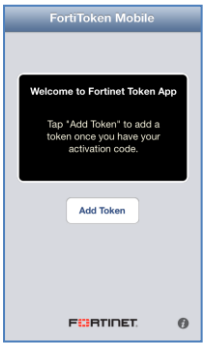
The FortiAuthenticator administrator should able to view the view the activation code from the interface under *Logging* > *Log Access* > *Logs*, as seen below

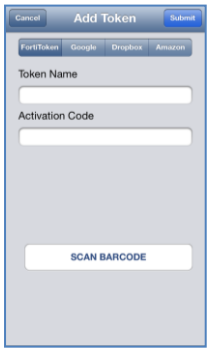


FortiToken Mobile for iOS

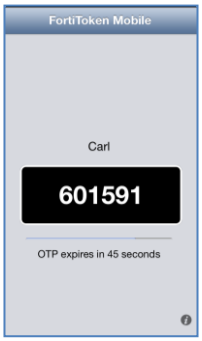
The next few steps address the FTM setup on an iOS compatible device. Once the FortiToken Mobile Application has been downloaded and installed, open the application

Then the activation code prompt will then appear, Tap ***Add Token*** (if using the application for the first time a PIN will need to be created).





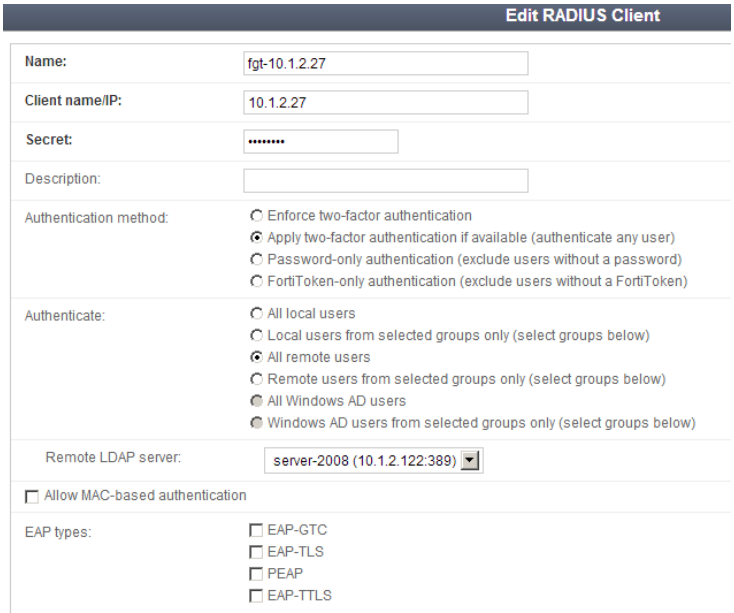
Then enter a token name and the activation code and *Tap **Submit***, if the code is valid, the application should start working immediately and begin prompting the passcode, as shown below.



The passcode prompt displayed by the FTM is used in the same manner as the FortiToken200 passcode prompt.

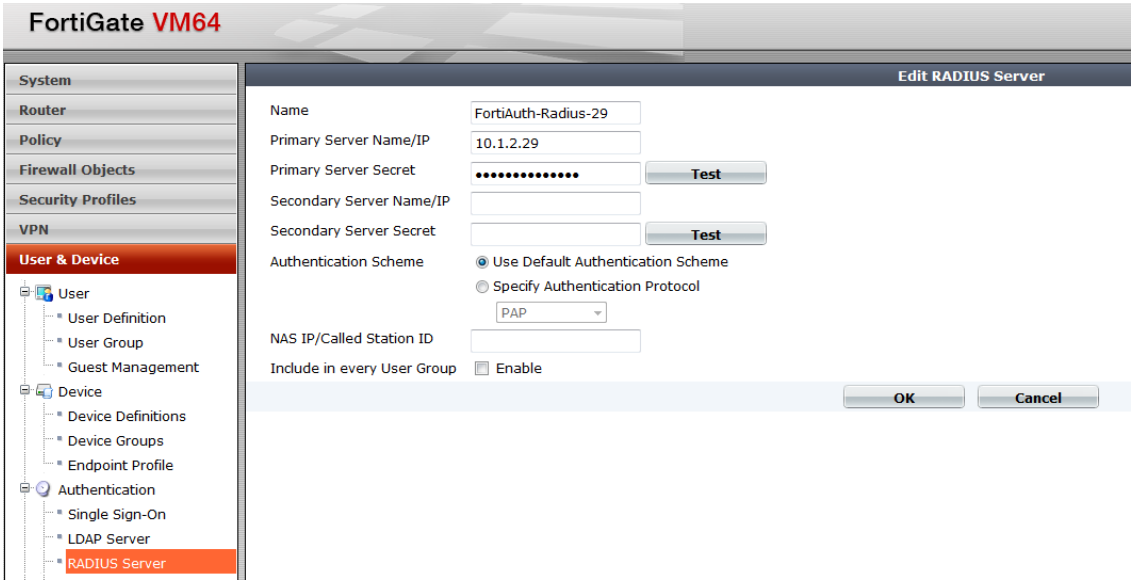
FortiAuthenticator RADIUS Client Configuration

The final FortiAuthenticator task is to define the FortiGate as a RADIUS client. Within the interface, go to *Authentication>RADIUS Service>Clients* and click on ***Create New***. Then enter the appropriate details (example below) and click on ***OK***.

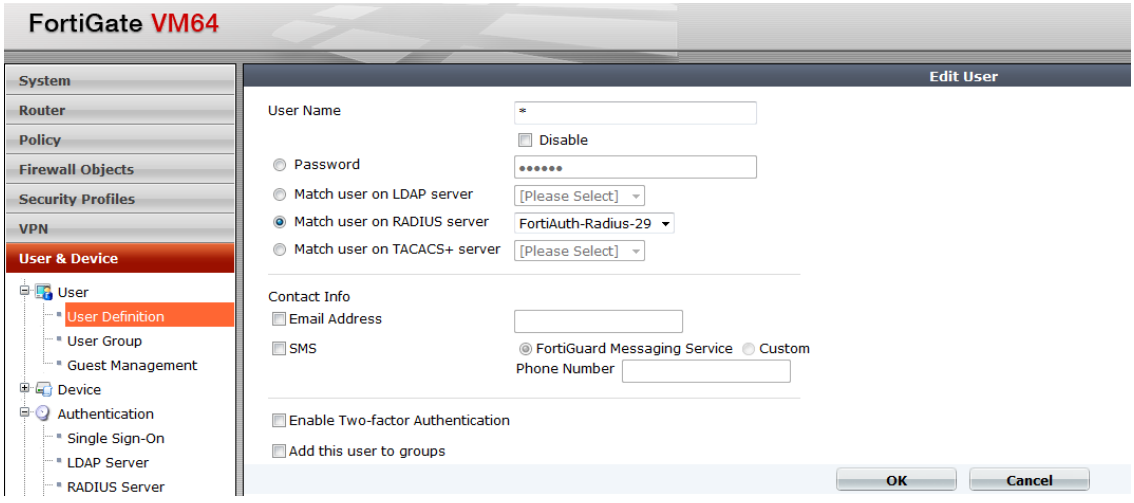


FortiGate RADIUS Client Configuration

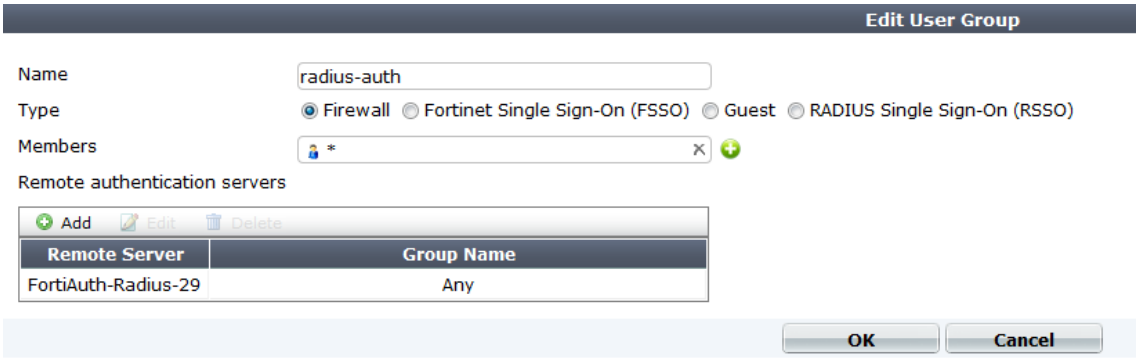
The next set of tasks will be carried out on the FortiGate. Initially the FortiGate needs to be configured as a RADIUS client to the FortiAuthenticator. Within the FortiGate interface, go to *User & Device* > *Authentication* > *RADIUS Server* and click on ***Create New***. Complete the RADIUS server details, and then test the connection, example below.



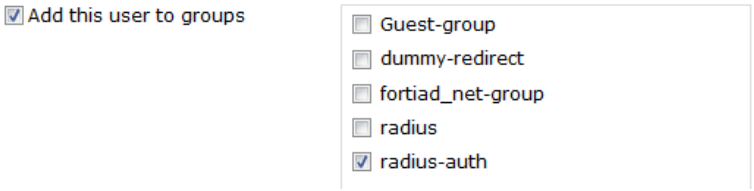
Next, a wildcard RADIUS user needs to be created. Go to *User & Device>User>User Definition* and click on ***Create New***. Then create a wildcard user as shown below. A wildcard user will allow the FortiGate to send all RADIUS authentication requests to the FortiAuthenticator.



The next RADIUS configuration step is to create the RADIUS group on the FortiGate which will be host the user(s) for the SSL VPN. Within the FortiGate interface go to *User & Device>User>User Group* and click on ***Create New*** and create a firewall authentication group that includes the wildcard user and references the FortiAuthenticator, example below.

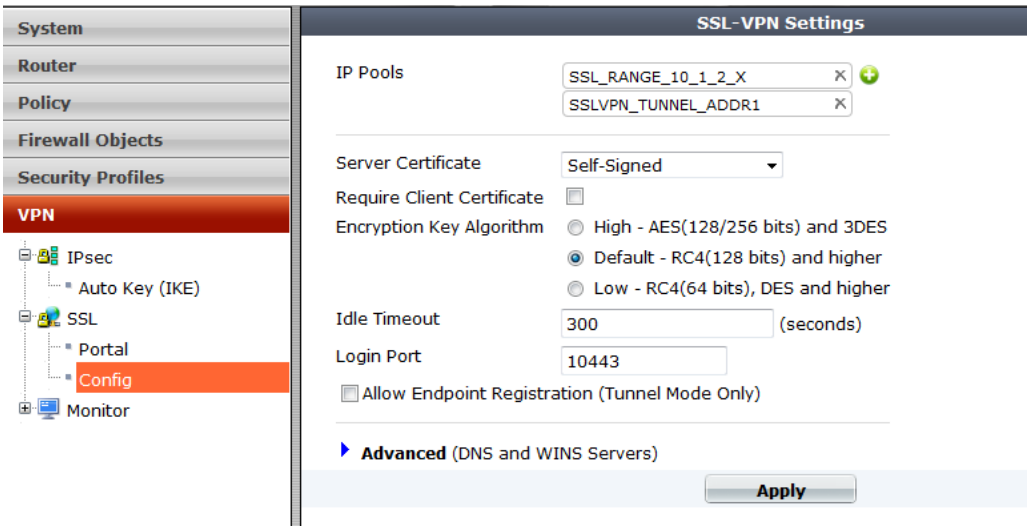


Then go back to the wildcard card user, *User & Device* > *User* > *User Definition* and add the wildcard user to the RADIUS group and ***OK*** the changes, example below.

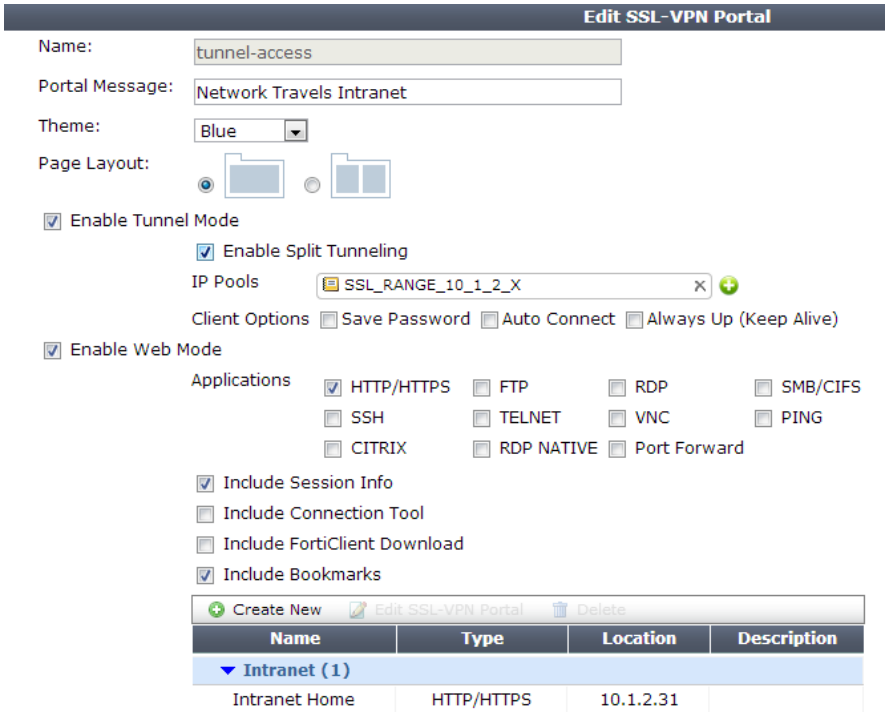


FortiGate SSL VPN Configuration

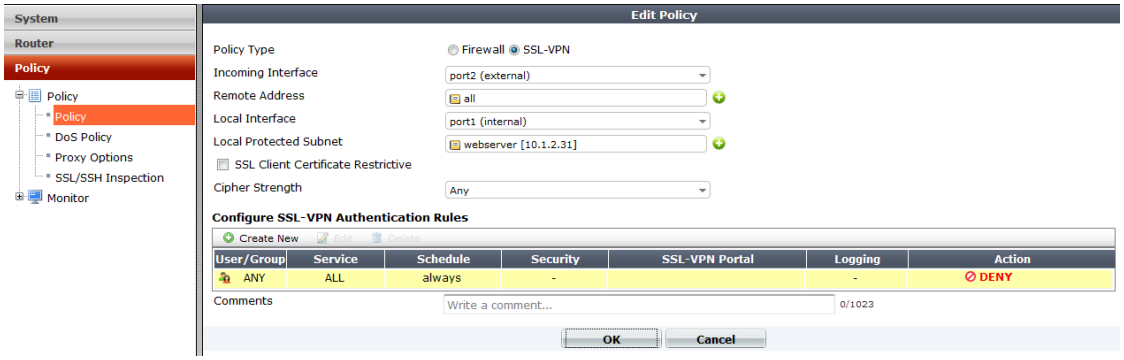
The following steps address SSL VPN creation on the FortiGate. Firstly ensure that there is a valid IP pool in place (under *Firewall Objects*>*Addresses*), if using an IP tunnel based VPN. To begin the SSL configuration, for both IP tunnel based and browser only VPN, go to *VPN*>*SSL*>*Config* and ensuring the relevant settings are in place, example below.



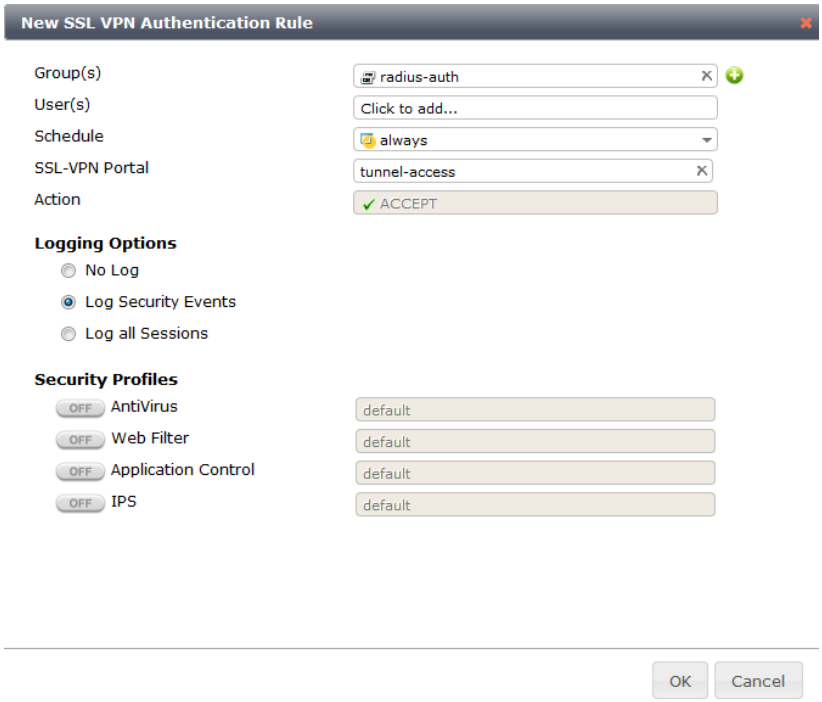
Then under *VPN* > *SSL* > *Portal* create the relevant SSL portal interface based on your VPN type (either *IP tunnel* or *browser only*), IP tunnel based VPN is shown in the example below.



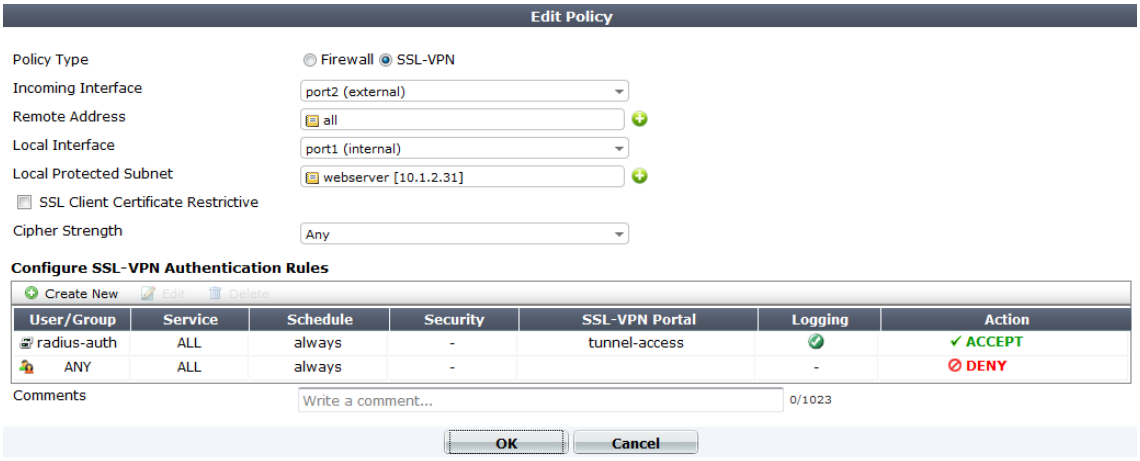
Within the FortiGate interface, go to *Policy* > *Policy* click on ***Create New,*** then click on VPN setup and create an external interface to internal interface SSL VPN policy, example below.



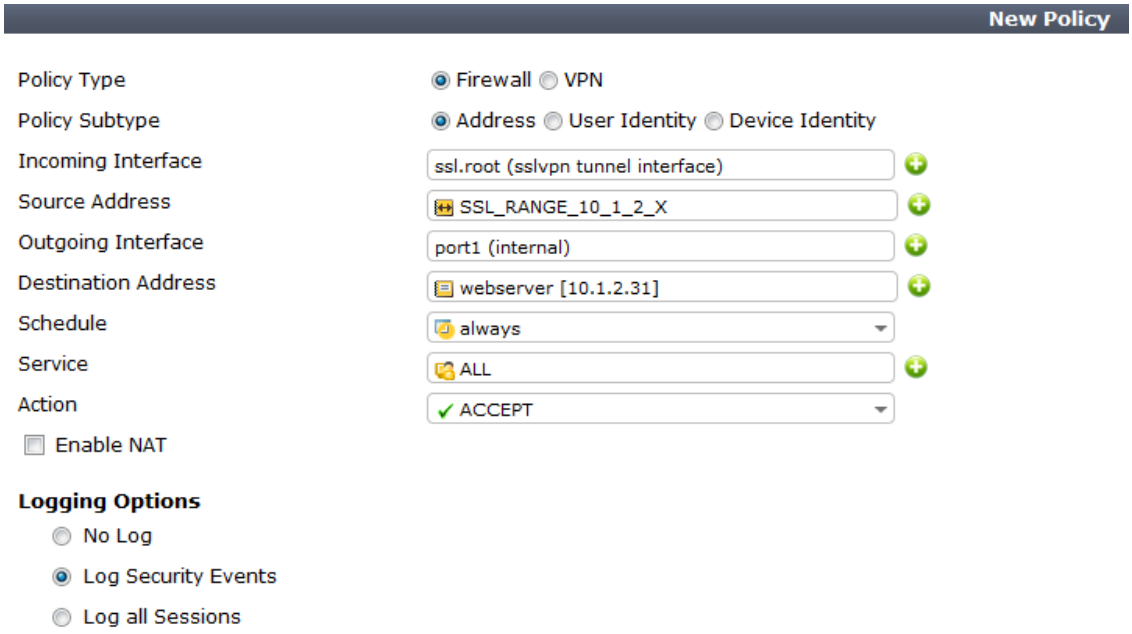
From within the policy configuration click on ***Create New*** under the '*Configure SSL VPN Authentication Rules*' section and use the preconfigured RADIUS group and the SSL VPN portal as in the example below, ***OK*** the changes and then ***OK*** the main policy.



If the completed SSL policy is selected and edited, the configuration should be as follows.



When configuring an IP tunnel SSL VPN (using the FortiClient), then an additional firewall policy is required (configured *Policy* > *Policy* and then ***Create New***), this is to allow incoming connections from the SSL tunnel interface to the internal network. An example of this is as follows.

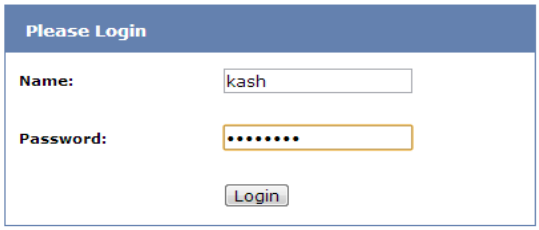


Once you OK the changes, the completed rule should look as follows in the policy section.

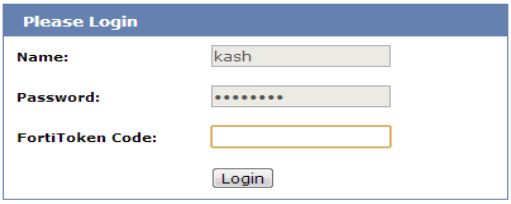
This completes the all configuration steps. It is now time to test the VPN.

Testing, Logging and Monitoring

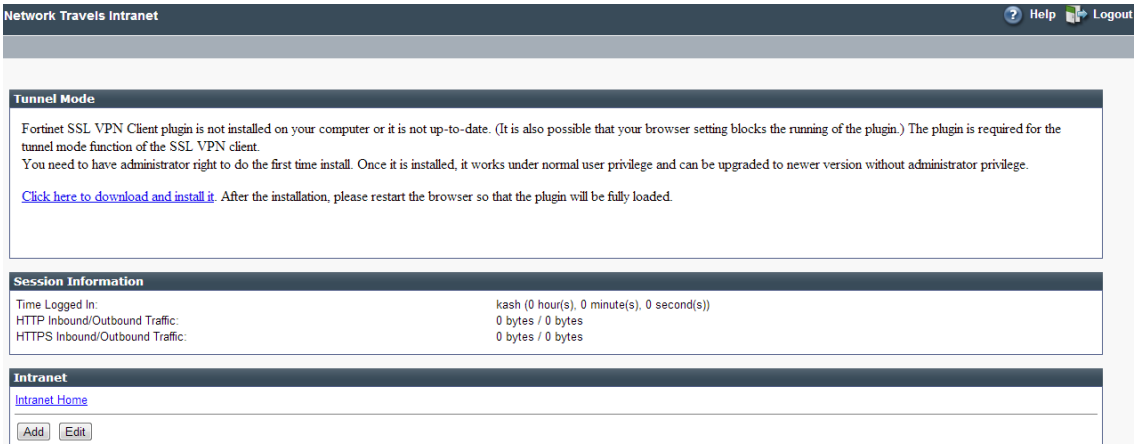
If the configuration is for a browser only SSL VPN, then open a browser to the SSL VPN gateway. Upon connecting to the gateway, the remote user will land on the standard SSL VPN login page, as below. At the login prompt, enter the directory username and password and then press ***Login***.



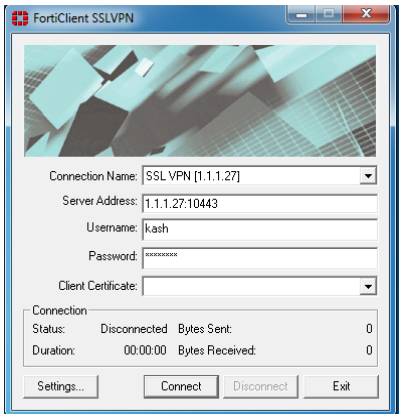
The remote user should then be prompted for a token passcode, as below. Enter the passcode from the FortiToken200 or FortiToken Mobile and click ***Login***.



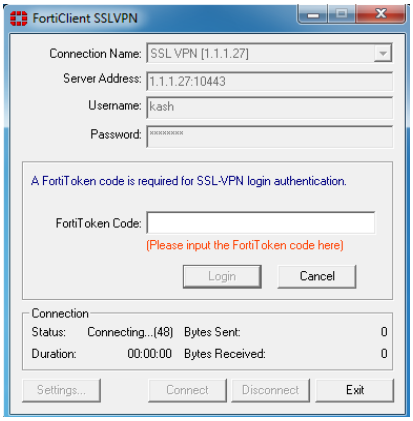
This should then successfully log the user on to the intranet, screenshot below. It is also possible to append the passcode on to the password in the initial login to prevent the passcode prompt.



If using FortiClient SSL, the open the client and complete the connection details and click on ***Connect***, example below.

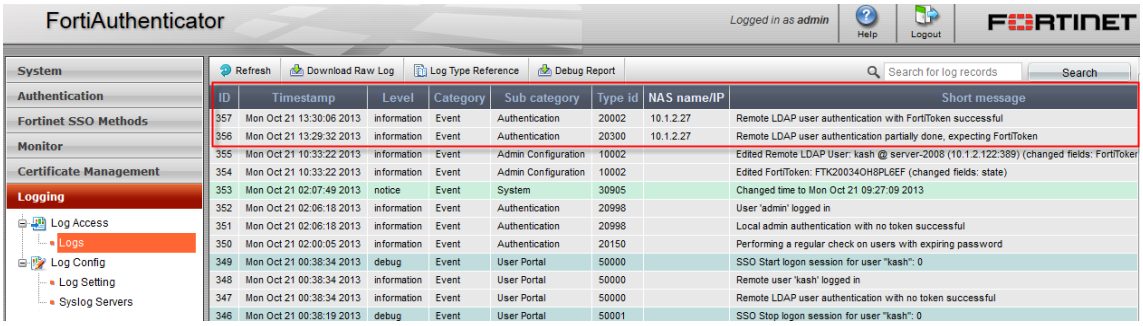


If the username and password is valid, the client will prompt for the token passcode (again this is either from the FortiToken200 or the FortiToken Mobile). If the passcode is correct, the VPN will commence the secure connection.



As with browser based authentication, it is possible to append the token passcode to the initial password to skip the secondary prompt.

Within the FortiAuthenticator user interface, under *Logging* > *Log Access* > *Logs* the following entry indicates successful token authentication.



This completes and confirms the Two-Factor SSL VPN Authentication testing, if the login is unsuccessful the FortiAuthenticator logs should provide indicative information, for detailed debugging please refer to the admin guide.

Additional Benefits

- FortiAuthenticator can introduce Two-Factor authentication to an existing FortiGate install base with minimal disruption
- With an easy to use interface and rich feature set, customers can increase the security of existing SSL or IPSec VPNs
- FortiAuthenticator supports E-mail and SMS Two-Factor authentication as well as Tokens
- Useful in token vendor migration scenarios
- FortiAuthenticator Two-Factor authentication capabilities can be combined with its Certificate Management capability to provide a comprehensive BYOD solution
- Users and Groups can be auto-imported (based on rules) from the directory server
- Active Directory authenticated users can feed into the FSSO (Fortinet Single Sign-On) framework allowing Identity Based access control across the network